



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|-------------|----------------------|---------------------------|------------------------|
| 10/749,558 | 01/02/2004 | Hsiang-Tsung Kung | 6720.0110-01 | 8770 |
| 22852 | 7590 | 08/06/2007 | | |
| FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP 901 NEW YORK AVENUE, NW WASHINGTON, DC 20001-4413 | | | EXAMINER TRAN, ELLEN C | |
| | | | ART UNIT 2134 | PAPER NUMBER |
| | | | MAIL DATE 08/06/2007 | DELIVERY MODE PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary

Application No.

10/749,558

Applicant(s)

KUNG, HSIANG-TSUNG

Examiner

Ellen C. Tran

Art Unit

2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 16 May 2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1,3-38 and 40-81 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1,3-38 and 40-81 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- ☒ Notice of References Cited (PTO-892)
- ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- ☒ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date Jun'06 - Mar'07.
- ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date: _____.
- ☐ Notice of Informal Patent Application
- ☐ Other: _____.

Art Unit: 2134

1. This action is responsive to communication filed on: 16 May 2007 with acknowledgement of an original application filed on 2 January 2004, with acknowledgement that this application is continuation in part of application 10/609,586 which claims benefit of provisional application filed 23 May 2003.
2. Claims 1, 3-38, 40-81 are currently pending in this application. Claims 1 and 38 are independent claims. Claims 1, 3, 4, 35, 38, and 40, have been amended. Claims 74-81 are new. Claims 2 and 39 are canceled. Amendments to the claims are accepted.
3. The IDS submitted 29 January 2007, 6 March 2007, and 6 June 2006 has been considered.

Response to Arguments

4. Applicant's argument with respect to provisionally Double Patenting rejection under 35 U.S.C. 101 has been considered and the rejection is removed due to cancellation of application 10/609,586.

Applicant's arguments filed 16 May 2007 have been fully considered however they are moot due to new grounds of rejection, necessitated by amendment to the independent claims

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Art Unit: 2134

6. **Claims 1-5, 10-13, 15-17, 20, 21, 27, 38-42, 46-50, 52-54, 57, 58, 62, and 74-81**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter '744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter '695).

As to independent claim 38 “An authentication method comprising: storing on a personal authentication device (PAD) at least one CA public key, each public key associated with a certificate authority (CA); receiving one or more digital certificates; authenticating the one or more received digital certificates using the at least one stored CA public key; generating at least one service based on the one or more authenticated digital certificates” is taught in '744 col. 5, lines 52-65 “FIG. 3 is a block flow diagram of steps performed in accordance with one embodiment of the invention. As shown in FIG. 3, a Certified Authority (CA) distributes smart card 10 to a user at step 50. Smart card 10 stores user information provided by the CA, such as tokens, digital signatures, certificates, tickets, PIN, human resources identification number, and so forth, or personal information provided by the user such as a social security number, birth date, mother's maiden name, etc. Smart card 10 also performs data encryption and decryption functions, stores DES secret keys and digital certificates, and will generate and store public and private RSA cryptographic key pairs. Smart card 10 has an on-board math co-processor that performs the key generation and encryption/decryption calculations”, note the PAD is interpreted to be equivalent to a smart card;

“and outputting the at least one service key” is shown in '744 col. 7, lines 22-28, “It is worthy to note that the specific data being stored and retrieved from the smart card in this example of a smart card interface module is in the form a user's social security number (SSN) for

use in authenticating the user. It can be appreciated, however, that any type of data could be stored or retrieved from the smart card, such as tickets, certificates, public/private keys, and so forth” note the Examiner interprets the other data to be equivalent to a ‘service key’;

the following is note explicitly taught in ‘744: **“wherein the one or more digital certificates comprise at least one ticket-generation certificate including at least one service key generating program or information indicating at least one service key generating program”**

however ‘695 teaches “Further, in an embodiment of the data processing system of the present invention, the second memory device may store a plurality of different application programs corresponding to a plurality of different service codes, and also may store a plurality of issue certificates corresponding to a plurality of application programs” on page 4, paragraph 0040 and ‘695 indicates “A description will be given of the data processing system in which the parent card as the first memory device and the child card as the second memory device are used with reference to FIG. 1. In FIG. 1, first, a user 100 requests issue processing of a parent card 110 to a parent card (first memory device) management authority 130, and submits necessary information for a parent card issue to the parent card management authority 130. The parent card management authority 130 registers, for example, personal information submitted from the user, or personal information obtained from the other databases in its own management database. Also, the authority stores personal information, the other necessary data, and programs in a parent card, executes generation processing of the parent card, and issues the generated parent card 110 to the user. The parent card 110 stores user personal information, an application program which controls issue processing of a child card (second memory device), and an issue-history registration table as a child card issue-management table. Furthermore, the card stores

public-key system key data, that is, a public key, a private key, a public-key certificate, etc. The data structure and the like in the card will be described in detail in the below. The user 100 who has received the parent card 110 issued by the parent-card management authority 130 can perform issue processing procedure of child cards 121 and 122 based on the received parent card 110. The child cards 121 and 122 are cards which are applicable to various services, for example, electronic money, hospital medical care cards, commuter's ticket for railroads and buses, etc., and is carried in a daily life" on page 8, paragraphs 0142-0143, note the processing in the second memory which executes a service such as issuing child cards or use the parent card for various services such as commuter's ticket for railroad or buses is interpreted to be equivalent to applicant's description of services provided in applicant's specification in paragraph 0050 frequent flyer or a member of an airline club.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card taught in '744 to include a means to utilize the smart card for services. One of ordinary skill in the art would have been motivated to perform such a modification because user authentication protocols suffer from weakness due to exposure see '695 (page 1, paragraphs 0010-0012). "IC cards have various use forms, for example, an above-described medical care card used in a hospital, an employee-ID card used in an organization such as a company, a commuter's ticket, etc. in addition to an electronic money described above. Thus, the processing executed on an IC card differs depending on the service providing entity (service provider) which provides each service. The application programs necessary for these processing are stored in a memory in an IC card, and when accessing a reader/writer under the control of each service provider, each program is executed to read or

write data stored in the IC card. A memory card, which stores such various data and are capable of executing various applications, stores various personal information as described above. Each service requires different personal information. If one piece of card is formed to be used for all the services, the card becomes necessary to store various personal information, such as a bank account number, an employee-ID number, or a medical history in addition to every personal information, for example, an address, a name, a telephone number, etc. Accumulation of personal information in such a way causes a problem of external exposure of personal information in the case of a card loss or a theft. Also, in recent years, crimes or illegal procedures using cards, in which a person who is not authorized for acquiring a legitimate card receives the card by pretending a legitimate card acquiring person by making a card issue request using an illegal procedure, etc., have been increased”.

As to dependent claim 40, “further comprising: authenticating the at least one received ticket-generation certificate using the at least one CA public key; and if the at least one ticket-generation certificate is authenticated, generating at least one service key based on the at least one service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service” is shown in ‘744 col. 5, lines 52-65.

As to dependent claim 41, “further comprising: receiving a user-identification certificate comprising information uniquely associated with a user; authenticating the received user-identification certificate based on the at least one CA public key; and if the user-identification certificate is authenticated, authenticating the user based on the authenticated user-identification certificate” is disclosed in ‘744 col. 5, lines 52-65.

As to dependent claim 42, “further comprising: receiving at least one user-qualification certificates indicating at least one service and one or more users who may access the at least one service; authenticating the at least one received user-qualification certificate based on the at least one CA public key; and if the at least one user-qualification certificate is authenticated, determining at least one service that the authenticated user may have access to based on the at least one authenticated user-qualification certificate” is taught in ‘744 col. 5, lines 52-65.

As to dependent claim 46, “storing on the personal authentication device (PAD) a PAD private key associated with the PAD” is shown in ‘744 col. 5, lines 52-65.

As to dependent claim 47, “further comprising: receiving a PAD authentication request; responding to the PAD authentication request using the stored PAD private key; and outputting the response to the PAD authentication request” is disclosed in ‘744 col. 5, lines 52-65.

As to dependent claim 48, “further comprising: signing the at least one service key using the stored PAD private key” is taught in ‘744 col. 5, lines 52-65.

As to dependent claim 49, “further comprising: decrypting contents on the one or more received digital certificates using the stored PAD private key, wherein the contents are encrypted with the corresponding PAD public key” is shown in ‘744 col. 5, lines 52-65.

As to dependent claim 50, “further comprising: if the authenticated user is determined to have access to the services, authenticating the at least one ticket-generation certificate using the at least one CA public key; and if the at least one ticket-generation certificate is authenticated, generating at least one service key based on the at least one

service key generating program, wherein the at least one service key may be used by a user to obtain access to at least one service” is disclosed in ‘744 col. 3, lines 31-45 and col. 5, lines 52-65, note the smartcard is used to generate the required access codes.

As to dependent claim 52, The method of claim 41, further comprising: receiving one or more received user credentials; and authenticating the user based on the authenticated user-identification certificate and the one or more user credentials” is shown in ‘744 col. 5, lines 52-65.

As to dependent claim 53, “wherein the user credentials comprise one or more user private keys” is disclosed in ‘744 col. 5, lines 52-65.

As to dependent claim 54, “wherein the user credentials comprise a personal identification number (PIN) associated with the user, or information computed from the PIN” is taught in ‘744 col. 4, lines 15-27 “Information from the card is accessed using the program and a PIN, and is compared with server information. Access to the web site will be either allowed or denied based upon the results of the comparison”.

As to dependent claim 57 “further comprising: receiving an operations certificate comprising information for controlling the operations of the PAD for a current session” is shown in ‘744 col. 6, line 64 through col. 7, line 10, note ability of the user to modify data stored on the smartcard is interpreted to be equivalent to controlling the operations of the PAD.

As to dependent claim 58, “wherein the information for controlling the operations of the PAD for a current session comprises one or more of the following: information governing input and output of the PAD, challenge and response protocols for user and PAD authentication, secure protocols for receiving and outputting data, and protocols for

PAD management purposes” is disclosed in ‘744 col. 6, line 64 through col. 7, line 10, note the user ability to change data is a management function.

As to dependent claim 62, “wherein at least one of the one or more digital certificates is received from a storage medium or network interface” is taught in ‘744 col. 3, lines 31-45, note the client computer has a reader for communicating with the card the computer has an interface to the network.

As to dependent claim 78, “wherein the at least one ticket-generation certificate further indicates a length of the at least one service key” is shown in ‘744 col. 10, lines 28-35.

As to dependent claim 79, “wherein the at least one ticket-generation certificate further indicates a format for outputting the at least one service key” however ‘695 indicates that the service key or authorization to use services can be used by a parent or child card on page 8, paragraph 0143, note utilizing the parent card for various services and generating child card is interpreted to be a ‘format’ of outputting a service key. The motivation to combine ‘744 and ‘695 is the same as stated above in independent claim 38.

As to dependent claim 80, wherein the information indicating the at least one service key generating program includes information of the at least one service key generating program stored on the PAD” however ‘695 indicates a service key generating program on page 4, paragraph 0040. The motivation to combine ‘744 and ‘695 is the same as stated above in independent claim 38.

As to dependent claim 81, “wherein the information indicating the at least one service key generating program includes information of the at least one service key

generating program available via one or more input devices” however ‘695 teaches on page 8, paragraphs 0144-0146, that each service provider, is an entity equipped with a child-card issue machine, the machine has one or more input devices. The motivation to combine ‘744 and ‘695 is the same as stated above in independent claim 38.

As to independent claim 1, this claim is directed to a personal authentication device utilizing the method of claim 38; therefore it is rejected along similar rationale.

As to dependent claims 2-5, 10-13, 15-17, 20, 21, 27, and 74-77, these claims contain substantially similar subject matter as claim 39-42, 46-50, 52-54, 57, 58, 62, and 78-81; therefore they are rejected along similar rationale.

7. **Claims 6, 9, 18, 22-23, 43, 51, 55, 59, 60, and 66**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter ‘744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter ‘695) in further view of de Jong et al. US Patent No. 7,085,840 (hereinafter ‘840).

As to dependent claim 43, the following is not explicitly taught in ‘695 and ‘744: **“wherein the at least one service key comprises at least one cookie”** however ‘840 teaches **“FIG. 50 is a block diagram that illustrates using a smart card to securely store and reconfigure cookies in accordance with one embodiment of the present invention”** in col. 10, lines 20-23.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card taught in ‘744 and ‘695 to include a means utilize cookies to distribute service keys. One of ordinary skill in the art would have been motivated to perform such a modification because the advent of the WWW has made more information available to use see ‘840 (col. 2, lines 24 et seq.). “The advent of the World Wide

Web (WWW) has made much more information available for use by anyone with a computer having an Internet connection. Unfortunately, current methods make it relatively easy to identify a particular user with specific data about the user, thus raising privacy concerns". In addition '744 was cited as a prior art reference by the Inventors of '840.

As to dependent 51, "wherein the one or more input means further receives one or more certificates comprising information for granting the user access to at least one additional service based on the at least one service" however '840 teaches "According to one embodiment of the present invention, a first credential is used to make a new credential having a more limited scope. For example, a first credential that grants access to view a web page or information unit may be used to create a second credential that provides access to a second Web page directly referenced by the first Web page for only 10 minutes. The same first credential might be used to create a third credential that provides access to any other Web pages referenced directly from the current Web page. More examples of using one or more credentials to create another credential are presented below with reference to FIG. 39" in col. 16, lines 1-13

As to dependent claim 55, "wherein the user credentials comprise biometric information associated with the user" however '840 teaches the use of biometrics in col. 15, lines 29-36.

As to dependent claim 59, "wherein the information for controlling the operations of the PAD for a current session comprises information governing linking of one or more received certificates, and wherein the method further comprises: linking one or more received certificates based on one or more certificates comprising information for granting

Art Unit: 2134

the user access to at least one additional service based on the at least one service” however ‘840 teaches linking the certificates in col. 16, lines 1-13

As to dependent claim 60, “further comprising: receiving one or more signature-verification certificates forming a signature-verification chain, wherein each signature-verification certificate in the signature-verification chain is signed with the private key of an entity whose public key is certified by the preceding signature-verification certificate and wherein the first signature-verification certificate in the signature-verification chain is signed by at least one stored CA public key; and wherein the processing component comprises at least one component for authenticating the one or more received digital certificates based on the last signature-verification certificate in the signature-verification chain” however ‘840 teaches the preceding key can be used to generate the next key in col. 16, lines 1-13.

As to dependent claim 66, “further comprising determining the number of times an event has occurred since a prior event” however ‘840 teaches a user profile is maintained based on the number of times a user visits a site, this is considered equivalent to a ‘prior event’ in col. 18, line 33 through col. 19, line 17.

As to dependent claims 6, 9, 18, 22, 23, these claims contain substantially similar subject matter as claim 43, 51, 55, 59, and 60; therefore they are rejected along similar rationale.

8. **Claims 7, 8, 44, and 45,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter ‘744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter ‘695) in further view of de Jong et al. US Patent No.

7,085,840 (hereinafter '840) in further view of Chang et al. US Patent No. 6,715,082 (hereinafter '082) in further view of Yu et al. US Patent No. 6,067,621 (hereinafter '621).

As to **dependent claim 44**, the following is not explicitly taught in the combination of teaches of '744, '695 and '840: **"further comprising: generating a one-time key and storing it on the PAD; based on the one-time key, generating the at least one cookie and sending the generated cookie to the user; receiving the previously generated the at least one cookie, and validating the received cookie using the stored one-time key"** however '082 teaches "One feature of this aspect is that the identification information includes a username and a one-time password (OTP); and the step of determining whether the session between the client and the first server should be established comprises the step of the first server communicating with a second server to determine whether the OTP is currently valid. According to another feature of this aspect, the step of communicating with a second server to determine whether the OTP is currently valid further includes the steps of the second server determining whether the username and the OTP were previously cached in memory; and if the username and the OTP were not previously cached in memory, the second server communicating with a password server to determine whether the OTP is currently valid" col. 3, lines 35-49, note the Examiner interprets the OTP equivalent to a one-time key.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card that utilizes cookies taught in '744, '695 and '840 to include a means utilize one time keys. One of ordinary skill in the art would have been motivated to perform such a modification to reduce security risks while communicating over a network see '082 (col. 2, lines 11 et seq.). "One method of reducing the security risks that are

Art Unit: 2134

introduced by fixed user identification information is through the use of a Smart card or Token card. One type of Token card, the SecurID card commercially available from Security Dynamics, Inc., continually generates a series of random one-time passwords (OTPs) that can be used once to login into a network access server. The Token card works in conjunction with a password server, such as Security Dynamics' ACE password server, and generates a response that is unique for every login. Because the password server generates a unique response for every login attempt, the OTP may only be used once to establish a session. Thus, even if monitored or stolen, the one-time password cannot be reused by an intruder to gain access to a user's account". the following is not explicitly taught in the combination of teachings in '744, '840, and '082:

"and if the received cookie is successfully validated, invalidating the one-time key used in the cookie validation, generating a new one-time key and store it on the PAD, and based on the new one-time key, generating a new cookie and sending the new cookie to the user" however '621 teaches "The portable terminal uses a card receiver for receiving the IC card to determine whether the IC card is input for the first time, a random number memory for reading and storing, and then deleting the random numbers of the IC card when the IC card is inserted for the first time into the card receiver, a first password generator for generating a one-time password by reading the secret key of the IC card and the random number stored in the random number memory, a first random number changer for changing the random number stored in the random number memory into a predetermined value and storing the changed value in the random number memory when a one-time password is generated in the first password generator, and a display for displaying the processed results of the terminal and the server." in col. 3, lines 27-42.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card that utilizes cookies and one-time keys taught in '744, '840, 605 and '082 to include a means update the key. One of ordinary skill in the art would have been motivated to perform such a modification to provide greater security see '621 (col. 2, lines 1 et seq.). "To provide greater security to user authentication, a one-time password may be used in which the password is changed each time the user wishes to be authenticated. In this method, an unauthorized person cannot reuse a password he or she found or stole from an authorized user because the password is changed each time the user wishes to be authenticated. In order to authenticate the identity of the user using the one-time password, a mechanism used to generate a one-time password is necessary. If every user uses a terminal of his or her own for generating the one-time password, security is enhanced because it is now possible to simultaneously confirm what only the user knows and what only the user owns in order to authenticate the user". In addition all the prior art references pertain to common subject matter of utilizing smartcards, token cards, or IC card.

As to dependent 45, "wherein the content in the one or more cookies comprises usage counts indicating the number of times one or more users have used one or more services" however teaches "According to one embodiment of the present invention, a Web site maintains a profile for the user. One exemplary use of a profile is to track the activity of a user at a particular Web site. The profile maintains information regarding the nature of the user activities with Vendor A 1806. For example, the profile may maintain information regarding the frequency of visits, the items previously purchased, the items examined but not purchased, the preferred shipping method and the preferred payment method, allowing Vendor A 1806 to

provide intelligent services tailored to the buying pattern of a particular user data set ...

According to one embodiment of the present invention, user data required to obtain a new service is obtained by dynamically combining the request for new service with at least one user data set obtained from a previous enrollment. For example, a user that shops at a first book vendor Web site may exhibit one or more preferences for books belonging to certain categories, based both on the books purchased at the Web site and on the books examined but not purchased. The first book vendor may save this information in a profile. The user may want to use all or part of this information when the user shops at a second book vendor Web site. Accordingly, a service request made by the user for service at the second book vendor Web site is automatically combined with the profile information used when shopping at the first book vendor Web site, thus creating a new profile for use by the user when shopping at the second book vendor Web site ” in col. 18, line 33 through col. 19, line 17, note the profile, which contains a usage count is sent with the cookie.

As to dependent claims 7 and 8, these claims contain substantially similar subject matter as claims 44 and 45; therefore they are rejected along similar rationale.

9. **Claims 19, 24, 26, 56, 61** are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter ‘744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter ‘695) in further view of Teicher et al. US Patent No. 6,257,486 (hereinafter ‘486).

As to dependent claim 56, the following is not explicitly taught in ‘744 and ‘695:
“further comprising: disabling the PAD if one or more attempts to authenticate the user based on the authenticated user-identification certificate and the one or more user

credentials ends in failure” however ‘486 teaches “Also important is an optional feature which disables the smart card if an invalid PIN is consecutively entered more than a predetermined number of times. The rationale for such a feature is that if a smart card is obtained by an unauthorized person, repeated attempts to guess the secret personal identification number by trial and error will most likely result in a series of invalid entries, which cause the smart card to be disabled. In some smart cards, the disabling can be reversed by the issuer (such as when the authorized user has merely forgotten the secret personal identification number), and in other smart cards the disabling is permanent and renders the smart card completely inoperative. The methods of authentication as used herein include the basic method as shown in FIG. 6 and described above, as well as any of these and other variations thereof” in col. 7, lines 10-23.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card taught in ‘744 and ‘695 to include a means to disable the smartcard. One of ordinary skill in the art would have been motivated to perform such a modification to improve the security of the smart cards see ‘486 (col. 10, lines 53 et seq. and col. 10, lines 24-38). “The limitations of the prior art discussed above detract from the security of smart card systems, and consequently undermine user as well as issuer confidence in the employment of smart cards. There is a recognized need for, and it would therefore be highly advantageous to have, a smart card and reader which better maintains security of the user's secret personal identification number and which does not suffer from these limitations, while at the same time preserving the appearance and utility of the commercial smart card as based upon the standards for integrated circuit cards. This goal is met by the present invention” and “The “SafePad” smart card reader is a compact device which has an internal authentication unit, and is

designed to be tamper-resistant. By performing user authentication within such a device, the problems indicated in FIG. 9B are intended to be minimized, because access to the internal components of the "SafePad" reader is harder to attain than access to the internal components and software of a personal computer. It is therefore intended by the manufacturer to be more difficult to compromise the user authentication process with the "SafePad" reader. Nevertheless, no device can be made completely tamper-proof, and so the "SafePad" reader merely isolates the problems indicated in FIG. 9B but does not completely eliminate them".

As to dependent claim 61, "further comprising: erasing the PAD private key when one or more unauthorized attempts to read or modify the PAD private key are detected" however '486 teaches "Furthermore, by having the authentication module normally disabled and enabled when presented to a reader, the possibility of a pre-authorization and the problems therefrom are removed" in col. 11, lines 14-21, note the Examiner interprets disabled equivalent to erasing.

As to dependent claim 24, the following is not explicitly taught in '744 and '695: **"wherein the PAD is tamper-resistant"** however '486 teaches "Furthermore, by having the authentication module normally disabled and enabled when presented to a reader, the possibility of a pre-authorization and the problems therefrom are removed." in col. 11, lines 14-21; note the prior art problems being corrected are described in col. 10, lines 24-38 so that the memory is tamper-resistant.

As to dependent claims 19, 26, these claim contain substantially similar subject matter as claim 56, 61; therefore they are rejected along similar rationale.

Art Unit: 2134

10. **Claims 25, 36, 37, 72, and 73** are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter '744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter '695) in further view of Geer, Jr. et al. US Patent No. 6,192,131 (hereinafter '131).

As to dependent claim 25, the following is not explicitly taught in '744 and '695:

“wherein the CA public keys and the PAD private key are written into the PAD only once”

however '131 teaches that smart cards are initialized once by writing private/public keys in col. 2, lines 40-50.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card taught in '744 and '695 to include a means to write encryption keys public/private only one to the PAD. One of ordinary skill in the art would have been motivated to perform such a modification to utilize smart cards for authorizing a user in transactions see '131 (col. 2, lines 26 et seq.). “With reference to FIG. 1, a system for implementing a transaction in accordance with the present invention includes an authorizing computer 10, a smart card 12 at authorizing computer 10 that corresponds to a specific user of the authorizing computer 10, an authorized computer 14 that is authorized by authorizing computer 10 to perform some specific action, and a transaction computer 16 that performs a transaction with authorized computer 14 that includes the authorized computer 14 performing the authorized action. The system also includes a certifying authority 18 that performs the conventional function of certifying the identity of the user to authorized computer 14 and transaction computer 16”.

As to dependent claim 72, further comprising: generating the at least one service key based on a write-once serial number” however ‘131 teaches “The authorizing computer also creates an identification certificate for the smart card at the authorizing computer and sends it to the authorized computer signed with the private key of the user of the smart card (step 27), and the authorized computer verifies the authenticity of the signature on the identification certificate (step 28) using the public key of the user of the smart card at the authorizing computer, which was received by the authorized computer in step 20. The private key of the identification certificate for the user of the smart card will be used for encryption (sealing) purposes and the private key of the identification certificate for the smart card itself will be used for signing purposes. In alternative embodiments it is possible to switch the roles of these private keys” in col. 3, lines 3-15, the serial number is interpreted equivalent to the identification certificate for the smart card.

As to dependent claim 73, “further comprising: including the serial number in the at least one service key” however ‘131 teaches the serial number sent with the key generated by the smartcard in col. 3, lines 3-15.

As to dependent claims 36 and 37, these claims contain substantially similar subject matter as claims 72 and 73; therefore they are rejected along similar rationale.

11. **Claims 28-31, 34, 63-65, 67, and 68,** are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter ‘744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter ‘695) in further view of de Jong et al. US Patent No. 7,085,840 (hereinafter ‘840) in further view of Chang et al. US Patent No.

6,715,082 (hereinafter '082) in further view of Yu et al. US Patent No. 6,067,621 (hereinafter '621) in further view of Baird, III et al. US Patent 6,732,278 (hereinafter '278).

As to dependent claim 63, the following is not explicitly taught in the combination of teaching of '744, '695, '840, '082, and '621: **"further comprising determining a current date and time"** however '278 teaches "A more sophisticated smart card includes a small screen that displays a different pseudorandom number at a given frequency, once every minute, for instance. The user reads the number from the smart card and types it into the device to which access is desired. The number serves as a password, albeit one that is changed frequently, to the device. The password is based on the current date and time, and the device and the smart card are date/time synchronized" in col. 1, line 65 though col. 2, line 8.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card that utilizes cookies and updatable one-time keys taught in '744, '840, '695, '082, and '621 to include a means utilize current date and time. One of ordinary skill in the art would have been motivated to perform such a modification to provide security easier see '278 (col. 2, lines 34 et seq.). "There is a need for an apparatus and method that can securely authenticate a user to existing online services, without requiring modifications to the current access process in use by those services, including especially the process for logging on to the site. Further the user should be able to conduct the transaction in a secure environment to ensure that transaction is in fact executed as desired". In addition all the prior art references pertain to common subject matter of utilizing smartcards, token cards, or IC card to access the network resources.

As to dependent claim 64, “further comprising: determining if the current date and time is within the validity period of the one or more received digital certificates” however ‘278 teaches “At the step 705, the device 101 sends the user identification and computer-generated password to the site 105 through an encrypted channel as discussed above. In one example secure sites are accessed using the secure sockets layer encryption scheme. A step 706 controls the password change process. The triggering events or change frequency for the site passwords are stored in the preferences database 408. The password can be changed at a predetermined frequency (e.g., weekly, monthly) or every time the user logs in to the account. Changing the site password at each log-on offers the highest level of security. In any case, if it is now time to change the password, the device 101 commands a site 105 to change the user's password to a new, randomly generated password. As discussed above, the new password can be generated based on the contents of the entropy pool 416. Once the password has been successfully changed, the process moves to a step 707 where access is granted to the account and the user's session with the account is controlled by a web browser or an operating system of the computer 103, for instance if the site 105 is a resource on a local area network. In one embodiment, the steps 706 and 707 occur nearly simultaneously so the process of changing passwords presents no perceptible delay to the user. As a result, it is not unreasonable to change the password at every log-in” in col. 19, lines 1-23.

As to dependent claim 65, “further comprising determining elapsed time since a prior event” however ‘278 that the password can be changed at each login, this is considered equivalent to a ‘prior event’ in col. 19, lines 1-23.

As to dependent claim 67, “further comprising: receiving one or more digital certificates which contain information for resetting current date and time, elapsed time, and a number of times an event has occurred” however ‘744 teaches the call functions can reset in col. 7, lines 35-40. The timers and counters are incorporated in a standard smartcard as shown by the prior art references.

As to dependent claim 68, “further comprising: resetting clock, timers or counters of the PAD based on information in the one or more digital certificates” however ‘744 teaches the call functions can reset in col. 7, lines 35-40 and that the client computer downloads control modules and certificates col. 5, lines 52-67. The timers and counters are incorporated in a standard smartcard as shown by the prior art references.

As to dependent claim 29, “further comprising one or more timers for determining time that has elapsed since a timer was reset” however ‘744 teaches the call functions can reset in col. 7, lines 35-40 and that the client computer downloads control modules and certificates col. 5, lines 52-67. The timers and counters are incorporated in a standard smartcard as shown by the prior art references.

As to dependent claim 31, “wherein the one or more digital certificates further comprise information which may reset clock, timers and counters of the PAD” however ‘744 teaches the call functions can reset in col. 7, lines 35-40 and that the client computer downloads control modules and certificates col. 5, lines 52-67. The timers and counters are incorporated in a standard smartcard as shown by the prior art references.

As to dependent claims 28, 30, and 31, these claims contain substantially similar subject matter as claims 63-65, 67, and 68; therefore they are rejected along similar rationale.

Art Unit: 2134

12. **Claims 32, 33, 35, and 69-71**, are rejected under 35 U.S.C. 103(a) as being unpatentable over Murphy et al. US Patent No. 6,226,744 (hereinafter '744) in view of Ishibashi et al. US Patent Publication No. 2004/0006695 (hereinafter '695) in further view of de Jong et al. US Patent No. 7,085,840 (hereinafter '840) in further view of Chang et al. US Patent No. 6,715,082 (hereinafter '082) in further view of Yu et al. US Patent No. 6,067,621 (hereinafter '621) in further view of Baird, III et al. US Patent 6,732,278 (hereinafter '278) in further view of Teppler US Patent 6,792,536 (hereinafter '536).

As to dependent claim 69, the following is not explicitly taught in the combination of teachings of '744, '695, '840, '082, 621, and 278: **“further comprising: receiving one or more digital certificates which provide a content decryption key and content rights; and checking the content rights before outputting the content decryption key as a service key”** however '536 teaches “Smart Card-enabled Signing of Active Content Smart cards can be used in conjunction with Authenticode technology to let end users identify who published a software component and verify that no one tampered with it before downloading it from the Internet. The first step for a developer is to acquire a software publishing certificate for use with Authenticode” and in col. 35, lines 9-23.

It would have been obvious to one of ordinary skill in the art at the time of the invention of a user authentication system using a smart card that utilizes current date and time, cookies and updatable one-time keys taught in '744, '840, '695, '082, '621, '536, and 278 to include a verify the content of data communicated. One of ordinary skill in the art would have been motivated to perform such a modification because a means is needed to verify the date and times associated with access and creation of files see '536 (col. 1, lines 32 et seq.). “Digital data files come in

many formats. None of those formats currently provide means for proving--with certainty--dates and times associated with access, creation, modification, receipt, or transmission of such digital data files. This is not only due to the variety of application programs which are available for digital data file access, creation, modification, receipt, and transmission, but also due to the much more varied "standards" and protocols put forth in the vain attempt to provide uniformity worldwide". In addition all the prior art references pertain to common subject matter of utilizing smartcards, token cards, or IC card to access the network resources, i.e. content.

As to dependent claim 70, "wherein the content rights comprise limits on at least one of the following: content expiration time, content usage period, content usage count" however '536 limits on content usage by time stamping in col. 35, lines 9-23.

As to dependent claim 71, "further comprising: generating timestamps based on the current date and time, the timestamps to be included in service keys that the PAD generates" however '536 limits on content usage by time stamping in col. 35, lines 9-23.

As to dependent claims 32, 33, 35, these claims contain substantially similar subject matter as claim 69-71; therefore they are rejected along similar rationale.

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a). A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened

Art Unit: 2134


statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (571) 272-3842. The examiner can normally be reached from 6:00 am to 4:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on (571) 272-3811. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

ET
Ellen Tran
Patent Examiner
Technology Center 2134
26 July 2007


KAMBIZ ZAND
SUPERVISORY PATENT EXAMINER